

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

Plaintiff,

v.

EVGENIY MIKHAILOVICH BOGACHEV,
et al.

Defendants.

Civil Action No.

14-0685

FILED *EX PARTE*
AND UNDER SEAL

RECEIVED

MAY 27 2014

CLERK, U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff, the United States of America has filed a complaint for injunctive relief pursuant
(*doc. no. 3*)
to 18 U.S.C. §§ 1345 and 2521, based on Defendants' violation of 18 U.S.C. §§ 1343, 1344, and
2511. The Government has also moved *ex parte* for a temporary restraining order and an order
(*doc. no. 4.*)
to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the
Federal Rules of Civil Procedures and 18 U.S.C. §§ 1345(a)(1) and 2521.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declaration, exhibits, and memorandum filed in support of
the Government's Motion for a Temporary Restraining Order, Order to Show Cause and Other
Ancillary Relief, the Memorandum of Law in support thereof ("Memorandum of Law"), as well
as the accompanying declaration, the Court hereby makes the following findings of fact and
conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good
cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim
upon which relief may be granted against Defendants under 18 U.S.C. §§ 1345 and 2511.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate 18 U.S.C. §§ 1343, 1344, and 2511, and that the Government is, therefore, likely to prevail on the merits of this action.

3. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of 18 U.S.C. §§ 1343, 1344, and 2511. The evidence set forth in the Government's Memorandum of Law, and the accompanying declaration, demonstrate that the Government is likely to prevail on its claim that Defendants have engaged in violations of 18 U.S.C. §§ 1343, 1344, and 2511 by:

- a. intentionally infecting hundreds of thousands of computers with malicious software ("malware") to steal banking and other online credentials from infected computers and enlist those computers into the Gameover Zeus "botnet" (a network of other infected computers controlled by the defendants);
- b. using the Gameover Zeus malware to intercept victims' communications without authorization;
- c. using credentials stolen by the Gameover Zeus malware to access victim bank accounts and fraudulently transfer funds; and
- d. intentionally infecting more than 100,000 computers in the United States with "Cryptolocker," a form of malware known as "ransomware," which encrypts users' critical files and then demands a ransom in order to return the files to a readable state.

4. There is good cause to believe that if such conduct continues, it will cause irreparable harm to both individuals and businesses in the United States. There is also good cause to believe that Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. Based on the evidence cited in the Government's Memorandum of Law and accompanying declaration and exhibits, the Government is likely to be able to prove that the Defendants are engaged in activities that violate United States law and harm members of the public, and that the Defendants have continued their unlawful conduct despite the clear injury to members of the public.

6. There is good cause to believe that providing the Defendants with advance notice of this action would cause immediate and irreparable damage to this Court's ability to grant effective final relief. Based on the evidence cited in the Government's Memorandum of Law and accompanying declaration, there is good cause to believe that – if the Defendants were to be notified in advance of this action -- the Defendants would relocate their servers and/or command and control infrastructure, change the coding of their malware, or otherwise implement measures to blunt or defeat the Government's planned disruption effort if informed in advance of the Government's actions.

7. The Government's request for this *ex parte* relief is not the result of any lack of diligence on the Government's part, but instead is based upon the nature of Defendants' illegal conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), good cause and the interests of justice require that this Order be granted without prior notice to Defendants, and accordingly, the Government is relieved of the duty to provide Defendants with prior notice of the Government's Application.

8. The Government has demonstrated good cause to believe that Defendants have directed their illegal activity at individuals and businesses located in the Western District of Pennsylvania by, among other things, infecting numerous computers in this District with Gameover Zeus and Cryptolocker and by using credentials stolen by the Gameover Zeus malware to gain unauthorized access to the bank accounts of victims in this District.

9. The Government has demonstrated good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from infecting computers with Gameover Zeus and Cryptolocker and from communicating with existing computers infected with Gameover Zeus and Cryptolocker.

10. The Government has demonstrated good cause to believe that Defendants have used, and will use in the future, the domain names identified in Appendix A to commit violations of 18 U.S.C. §§ 1343, 1344 and 2521 in connection with the Gameover Zeus malware. There is good cause to believe that to immediately halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current and prospective domains set forth in Appendix A must be immediately: 1) made inaccessible to the defendants; and 2) redirected to the following name-servers: ns1.kratosdns.net and ns2.kratosdns.net.

11. There is good cause to believe that Defendants have used, and will use in the future, the domain names identified in Appendix B to commit violations of 18 U.S.C. § 1343 in connection with the Cryptolocker malware. There is good cause to believe that to immediately halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current and prospective domains set forth in Appendix B must be immediately made inaccessible.

12. There is good cause to believe that Defendants have used, and will use in the future, the .ru domain names identified in Appendix C to commit violations of 18 U.S.C. §§ 1343, 1344 and 2521 in connection with the Gameover Zeus malware and violations of 18 U.S.C. § 1343 in connection with the Cryptolocker malware. There is good cause to believe that to immediately halt the Defendants' illegal activity and to prevent further harm to individuals and businesses in the United States, each of the Defendants' current and prospective .ru domains set forth in Appendix C must be immediately made inaccessible.

13. There is good cause to permit service of documents filed in this case that have been unsealed by this Court, and any unsealed Orders entered by the Court in response thereto, as provided below, given the exigency of the circumstances, and the need for prompt relief. The following means of service, which provide due process, satisfy Fed. R. Civ. P. 4(f)(3), and are reasonably calculated to provide notice to Defendants:

- a. Via overnight delivery upon defendant Bogachev's home address in Anapa, Russian Federation; and
- b. Via email to the email addresses used by defendant Bogachev and the defendant using the alias Chingiz 911 as identified in the Declaration of Special Agent Peterson;
- c. Via email to the email addresses provided by the registrants of all active Internet domain names currently used by the Defendants to control the malicious software programs known as Gameover Zeus and Cryptolocker; and
- d. Via publication on the Internet web sites of the Department of Justice and the Federal Bureau of Investigation.

Plaintiff shall promptly file an Affidavit of Service on ECF certifying conformity to para. 13.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular, are prohibited from running, controlling, or communicating with software known as Cryptolocker and Gameover Zeus (also known as Peer to Peer Zeus), on any computers not owned by the Defendants.

IT IS FURTHER ORDERED that the Government shall establish substitute server(s) and other computer infrastructure as specified in the Government's Memorandum of Law that, in conjunction with the relief ordered below, will replace the Defendants' command and control infrastructure for the Gameover Zeus botnet and sever the Defendants' connection to the infected computers in the Gameover Zeus botnet. Pursuant to the Pen Register Trap and Trace Order signed by this Court, the Government is authorized to collect dialing, routing, addressing and signaling ("DRAS") information from the infected computers that connect to the infrastructure created pursuant to this Order. The Government shall ensure that no electronic content or other non-DRAS information is collected when victim computers connect to the infrastructure established pursuant to this Order.

IT IS FURTHER ORDERED that, with respect to any currently registered domains set

forth in Appendix A, the Domain Registries identified in Appendix E shall take the following actions:

(doc. no. 6-5)

1. Take all reasonable measures to redirect the domains to the substitute servers established by this Order, including changing the authoritative name servers for the domains to ns1.kratosdns.net and ns2.kratosdns.net
2. Take all reasonable measures to propagate the foregoing changes through the Domain Name System as quickly as practicable;
3. Prevent any further modification to, or transfer of, the domains without the previous authorization of this Court;
4. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order;
5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any currently unregistered domains set forth in Appendix A, the Domain Registries identified in Appendix E shall take the following actions:

(doc. no. 6-5)

1. Take all reasonable measures to redirect the domains to the substitute server(s) established by this Order, including changing the authoritative name servers for the domains to ns1.kratosdns.net and ns2.kratosdns.net;
2. Take all reasonable measures to propagate the foregoing changes through the Domain Name System as quickly as practicable;

3. Prevent any further modification to, or transfer of, the domains without the previous authorization of this Court;
4. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order;
5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any currently registered domains set forth in Appendix B, the Domain Registries identified in Appendix E shall take the following actions:

(doc. no. 6-5)

1. Take all reasonable measures to render the domains unresolvable through the Domain Name System;
2. Take all reasonable measures to propagate the foregoing changes through the Domain Name System as quickly as practicable;
3. Prevent any further modification to, or transfer of, the domains without the previous authorization of this Court;
4. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order.
5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any currently unregistered domains set forth in Appendix B, the Domain Registries identified in Appendix E shall take the following actions: *(doc. no. 6-5)*

1. Take all reasonable measures to reserve, lock, or otherwise prevent the domains from being resolved;
2. If applicable, take all reasonable measures to propagate the foregoing changes through the Domain Name System as quickly as practicable;
3. Prevent any further modification to, or transfer of, the domains without the previous authorization of this Court;
4. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order;
5. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that with respect to the domain names set forth in Appendix C, the Internet Service Providers identified in Appendix D shall take reasonable best efforts to implement the following actions: *(doc. no. 6-4)*

1. Render the domains unresolvable by blocking domain name resolution for the domains;
2. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from disclosing this Order until such time as this Order is no longer under seal, except as necessary to execute this Order.

3. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants, Defendants' representatives, or any other person; and
4. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that copies of the Court Filings shall be served as follows:

1. via overnight delivery to the home address of Evgeniy Bogachev in Anapa, Russia;
2. via email to the known email addresses for defendants Evgeniy Bogachev and Chingiz 911;
3. via email and postal mail to each postal and email address provided by the registrants of all active Gameover Zeus and Cryptolocker domain names; and
4. via publication on the websites of the Department of Justice and the Federal Bureau of Investigation.

IT IS FURTHER ORDERED that pursuant to Federal Rule of Civil Procedure 65(b) *June 3, 2014 at 11:00 AM* that the Defendants shall appear before this Court on ~~June 3, 2014~~ to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on the Government any answering affidavits, pleadings, motions, expert reports or declarations *June 2, 2014 at 4:00 PM on ECF* and/or legal memoranda no later than ~~two (2) days prior to the hearing on the Government's request for a preliminary injunction.~~ The Government may file responsive or supplemental

pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than June 3, 2014 at 8:00 AM on ECF. ~~one (1) day prior to the preliminary injunction hearing in this~~
~~matter. Provided that service shall be performed by personal or overnight delivery, facsimile or~~
~~electronic mail, and documents shall be delivered so that they shall be received by the other~~
~~parties no later than 4:00 p.m. (Eastern Time) on the appropriate dates listed in this paragraph.~~

IT IS FURTHER ORDERED that this Order shall expire on the 3rd day of June 2014, at 2:00 ~~am~~ p.m. [~~not to exceed 14 days~~], subject to the further Order of this Court.

Entered this 28th day of May, 2014 at 9:48 a.m. ~~am~~


HON. ARTHUR J. SCHWAB
UNITED STATES DISTRICT JUDGE